한국항행학회 논문지 제17권 제2호 2013년 4월 (JKONI 17(2): 157-164, Apr. 2013)

이차원 C/A 코드 검색 공간에서의 이중피크 검출을 이용한 기만신호 대응 기법

Anti-Spoofing Method Using Double Peak Detection in the Two-Dimensional C/A Code Search Space

권금철*, 양철관*, 심덕선*

Keum-Cheol Kwon*, Cheol-Kwan Yang*, and Duk-Sun Shim*

요 약

일반적으로 기만신호는 GPS 신호보다 세기가 강한 신호이기 때문에 기만신호가 가해졌을 경우 GPS 신호의 정보를 획득하기는 어렵다. 특정 위성에 대한 기만신호가 발생하면 위성신호 획득시 도플러 주파수와 코드 페이스의 2차원 공간에 두 개의 피크가 존재하게 된다. 이를 이용하여 기만신호 존재 여부를 판단하고 각각의 신호획득 결과에 대한 채널 정보를 바탕으로 신호추적과정을 수행하여 기만신호를 제외한 GPS 신호를 활용할 수 있다. 본 논문에서는 의사위성 시뮬레이터를 이용하여 현재 가시위성 중 하나의 PRN에 대한 기만신호를 생성한 다음 소프트웨어 수신기를 이용하여 두 번의 신호획득 과정을 수행하여 두 개의 피크를 검출하고 각각에 대한 신호추적 이후 정상적인 GPS 신호의 결과를 추출할 수 있음을 확인하였다.

Abstract

In the presence of spoofing signal the GPS signal having the same PRN with the spoofer is hard to be acquired since the power of spoofing signal is usually stronger than that of GPS signal. If a spoofing signal exists for the same PRN, there are double peaks in two-dimensional space of frequency and code phase in acquisition stage. Using double peak information it is possible to detect spoofing signal and acquire GPS information through separate channel tracking. In this paper we introduce an anti-spoofing method using double peak detection, and thus can acquire GPS navigation data after two-channel tracking for the same PRN as the spoofing signal.

Key words : GPS, Pseudolite, Acquisition, Tracking, Spoofing, Software receiver.

I. 서 론

군사목적으로 개발되었던 GPS는 민간용 신호로 개방된 이후 활용도가 높아지면서 내비게이션, 이동통신 분야 등 여러 분야에서 사용되어 실생활에 있어서 아주 중요한 역할을 담당하고 있다. 하지만 GPS는 20,200km 상공에서 전송되는 위성신호로 세기가 -160dBW로 매우 낮기 때문에 여러 가지 전파 간섭의 영향을 받기 쉽다. 실제 2010년 이후 여러 차례에 걸쳐 GPS 전파교란이 발행하여 많은 피해가 발생하기도 하였다.

GPS 신호에 대한 전파교란은 크게 두가지 방식으

* 중앙대학교 전자전기공학부(School of Electrical and Electronics and Engineering, Chung-Ang University)
· 제1저자 (First Author) : 권금철(Keum-Cheol Kwon, Tel : +82-2-820-5321, email : casey518@naver.com)
· 접수일자 : 2013년 4월 2일 · 심사(수정)일자 : 2013년 4월 2일 (수정일자 : 2013년 4월 20일) · 게재일자 : 2013년 4월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.2.157

로 이루어지는데 재밍(jamming)에 의한 교란과 기만(spoofing)신호에 의한 교란으로 나누어 볼 수 있다. 재밍은 GPS 신호와 동일한 RF 주파수 대역의 신호를 GPS 신호보다 강한 세기로 발생시켜 GPS 수신기로 하여금 GPS 신호의 추적을 정상적으로 수행할 수 없도록 하는 방식이다. 재밍신호는 GPS보다 강한 신호를 전송해야 하기 때문에 오랜시간 동안 교란을 하기 어렵지만 광범위한 지역에 대해 영향을 줄 수 있다. GPS 수신기의 정상적인 기능 수행을 방해하는 재밍신호와 달리 기만신호는 수신기로 하여금 정상적으로 기능을 수행하면서 오동작을 유도하는 방식이다. 기만신호는 P코드 또는 Y코드로 암호화 되어 있는 군용 GPS신호와 달리 민간용 GPS의 신호구조가 공개되어 있다는 점을 이용하여 GPS 위성신호와 동일한 구조의 신호를 항법오차를 포함시켜 생성하여 수신기에 전송한다. 기만신호에 대한 구분이 되지 않으면 수신기는 실제 위성신호로 판단하여 잘못된 위치정보를 산출하게 된다. 재밍신호는 GPS 수신기의 신호추적 과정을 방해하기 때문에 재밍신호의 존재를 쉽게 감지할 수 있지만 기만신호는 수신기가 정상적인 동작을 수행하도록 하기 때문에 기만 여부에 대하여 판단하기 어려워 더 치명적인 결과를 초래할 수 있다. 현재 일반 GPS 수신기에는 기만신호에 대하여 대응하는 기능이 포함되어 있지 않아 이에 대한 감지 및 대응 기법에 대한 연구가 필요한 상황이다[1].

본 논문에서는 GPS 기만신호의 특성 및 대응법에 대하여 간략히 알아 보고 소프트웨어 수신기를 이용한 신호획득 단계에서의 이중피크 검출을 통한 기만신호 대응법을 제안하고 그 결과에 대하여 분석해 보고자 한다. 본 논문에서는 신호 획득 단계에서 두 개의 피크를 조사해서 기만신호의 존재여부를 판단하며, 두 개의 피크가 존재할 때에는 두 개의 추적 루프를 구동하여 GPS 신호를 사용할 수 있는 방법을 제안한다. 이 방법은 도시의 빌딩 협곡 같은 곳에서 가시 위성의 개수가 제한적일 때 유용하게 사용할 수 있다.

II. GPS 기만 신호의 특성 및 대응 기법

2-1 GPS 기만신호의 특성

기만신호는 GPS 신호와 동일한 구조를 가지면서 GPS 위성신호와 비슷한 세기의 신호로 수신되어야 한다. 신호 전력은 기만기와 수신기간의 거리의 영향을 크게 받기 때문에 일반적으로 수신기의 위치가 고정되었거나 이동 패턴이 일정한 지역이 기만의 주요 대상이 된다.

기만신호를 생성하는 방법으로는 가장 기본적으로는 GNSS 신호생성기를 이용하여 현재 GPS 위성과 시각 동기 없이 기만신호를 생성하는 방식이 있다. 그리고 GPS 위성의 신호와 동기를 맞춰서 기만신호를 생성하는 방식이 있는데 이를 위해서 GPS 신호를 처리하여 현재 가시위성에 대한 도플러 정보, 항법데이터, 신호 세기 등에 대한 정보를 추출하기 위한 수신기와 이를 이용하여 기만신호를 생성하기 위한 기만 신호 생성기로 구성된다[2].

2-2 기만신호 검출 및 대응 기법

일반적으로 GPS 수신기는 신호획득 단계에서 구성된 채널 정보를 이용하여 신호를 추적하게 된다. 신호추적을 불가능하게 하는 재밍신호와 달리 정상적인 신호추적 과정을 수행하게 하는 기만신호는 이에 대해 감지 및 대응하기 위한 알고리즘이 추가적으로 필요하다. 이를 위해 기만신호에 대한 감별과정이 우선적으로 수행되어야 하고 감별된 기만신호를 처리하는 과정이 진행된다. 신호 감별에는 수신기에서 수신되는 신호의 세기나 반송파, 도플러 주파수, 항법 메시지 등을 이용한 기법들이 사용된다.

신호세기를 이용한 기만신호를 검출하는 방법으로는 기만신호가 위성신호보다 강한 신호로 발생된다는 점을 이용하여 신호세기의 절대적인 값을 측정하여 감별하거나 신호 세기의 변화율을 이용하는 방법이 있다. 다중주파수 수신기의 경우 L1, L2C, L5의 상대적인 수신신호 전력값을 이용할 수도 있다. 반송파나 도플러 주파수를 이용한 방법으로는 신호추적 루프에서 코드와 반송파의 변화율을 보고 감별하는 방식과 도플러 주파수 변화량을 이용한 검출 방식이 있다. 그리고 전리층 효과에 의한 L1와 L2의 측정치를 비교하거나 코드와 반송파를 이용한 의사거리 측정치 변화율을 이용하여 감별할 수 있다. 이외에 여러 측정치에 대한 갑작스런 변화를 감시하여 감별하거나 위성 위치계산에 사용된 항법데이터를 비교하여 기만여부를 판별하는 방식도 있다[3].

기만신호가 판별이 되면 기본적으로 기만된 위성 신호의 채널 정보를 제거하고 항법해를 계산하는 과정에서 해당 위성 신호를 배제하는 방법으로 처리한다. 그리고 수신기의 안테나와 RF단에 추가적인 장비를 장치하여 검출된 기만신호의 PRN 신호에 대한 역 위상신호를 생성한 다음 기만신호를 상쇄시켜 기만신호를 극복하는 방법이 있다[4].

III. 이중피크 검출을 이용한 기만 신호 대응 기법

GPS 기만신호가 대상 수신기에 영향을 주는 시점은 수신기의 초기 동작 시점과 이미 신호추적을 하고 있는 도중의 시점으로 나누어 생각해 볼 수 있다. 신호획득 단계에서는 기만신호 정보를 가지고 채널 정보를 구성하여 신호추적과정을 수행하게 되고 GPS 위성에 대한 정상적인 신호추적을 수행하고 있는 수신기에 대해서는 기만신호의 코드지연이 1-chip 이내인 경우에만 영향을 받게 된다.

신호획득 단계에서 현재 가시위성과 동일한 PRN을 가진 기만신호가 인가된 상태라면 correlation값을 보면 두 개의 피크가 확인되고 일반적인 수신기는 이중에 큰 신호의 정보를 획득하게 될 것이다.

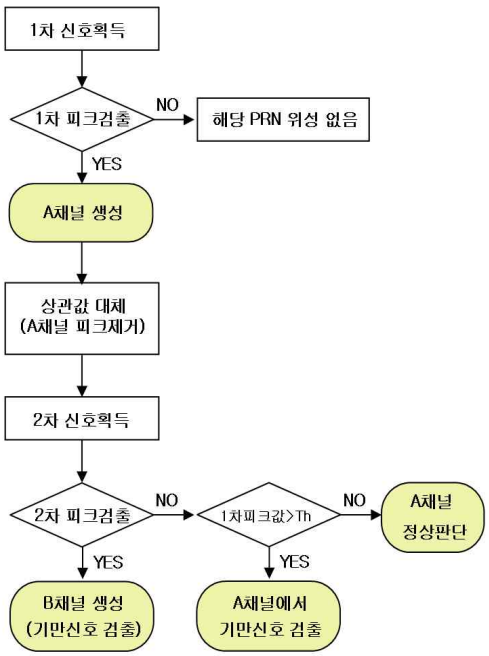


그림 1. 이중 피크 검출방법을 사용한 신호획득 과정
Fig.1. Signal Acquisition using Double Peak Detection

이때 상대적으로 작은 신호는 실제 GPS 위성 신호가 되고 이에 대한 신호획득 정보를 얻기 위하여 두 번째 피크를 찾는 과정을 신호획득 과정에 추가하였다. 기만 신호 검출은 그림 1과 같은 과정으로 진행된다.

1차 신호획득 과정에서 피크가 검출되면 신호획득 결과로 A채널을 생성하고 1차 피크의 주변값을 전체 correlaion 평균값으로 대체한 다음에 2차 신호획득 과정을 수행한다. 2차 피크가 검출되면 B채널을 생성한다. 1차 신호획득 이후에 첫 번째 피크의 앞뒤 1/2 chip 구간에 대해 상관값을 전체 평균값으로 대체하였기 때문에 GPS신호와 기만신호가 1 chip 이내로 동기 되어 있을 경우에는 2차 피크 검출시에 피크검출이 되지 않는다. 이러한 경우에는 추가적으로 GPS 신호에 비해 기만신호의 세기가 일정이상 큰 경우에 대한 판별값(Th)을 이용하여 기만신호 여부를 판단할 수 있다. 2차 피크검출이 이루어 지지 않았을 경우에는 1차 피크값과 판별값을 비교하여 1차 피크에서 검출한 신호가 기만신호인지 정상 GPS 신호인지를 판단하게 된다[3].

이 방식은 신호추적 이후 측정치나 궤도력 정보 등을 이용한 기만신호 검출 이후 해당 PRN을 제거하는 방식과 달리 각각의 피크에 대한 채널 정보를 생성하여 신호추적 과정을 수행할 수 있기 때문에 이후에 기만신호 판별 여부에 따라 해당 PRN에 대한 위성 정보를 획득할 수 있다.

IV. 실험 결과 및 분석

기만신호 생성을 위하여 GSG-L1 GPS 신호발생기를 사용하였으며 신호를 -110dBm 세기로 발생시켜 소프트웨어 수신기가 신호발생기와 GPS 위성 신호를 동시에 수신하여 신호획득, 신호추적 과정의 수행결과를 비교하여 기만신호의 영향을 확인하였다. 이때 기만신호 생성기에서 발생하는 신호의 세기가 GPS 신호의 전력레벨과 조금 크거나 조금 작은 상황에 대한 실험을 위하여 수신기와 신호발생기간의 거리를 변경시켜가며 실험을 진행하였다. GPS L1 신호는 2013년 2월 18일(PRN-10)과 19일(PRN-14) 중앙대학교 공과대학 제1공학관 옥상에서 샘플링 주파수

9MHz로 수신되었고 신호발생기와 동시에 수신한 신호를 기존의 소프트웨어 수신기의 신호획득 결과로 표1과 같이 7개의 위성이 획득되었다. 신호획득의 판단 기준이 되는 ratio값은 correlation 평균값 대비 피크값의 비율을 나타낸다.

표 1. GPS L1 신호획득 결과
Table 1. GPS L1 Acquisition Result

Sat	coarse_freq	fine_frequency	code_phase	ratio
2	2578000	2577879	3003	38.3
4	2580500	2580596	8275	42.7
5	2577000	2577124	40	34.1
10	2579500	2579573	2079	57.4
12	2581000	2581050	6286	14.8
13	2581000	2580901	5181	19.7
17	2583000	2582860	4307	30.9

GPS와 유사한 세기의 기만신호(PRN-10)가 가해졌을 때 신호획득의 결과로 두 개의 피크가 확인되는 것을 그림 2에서 확인할 수 있다. 수신기는 둘 중에 높은 피크값에 대한 정보를 가지고 채널을 생성하여 신호추적을 하게 된다. 그림 3은 상관값이 큰 왼쪽의 피크 신호를 추적한 결과로 신호추적이 정상적으로 수행되는 것을 확인할 수 있다.

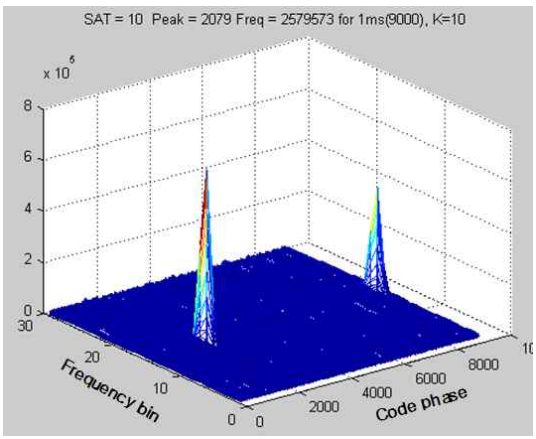


그림 2. 1차 신호획득 결과(PRN-10)
Fig.2. 1st Acquisition Result(PRN-10)

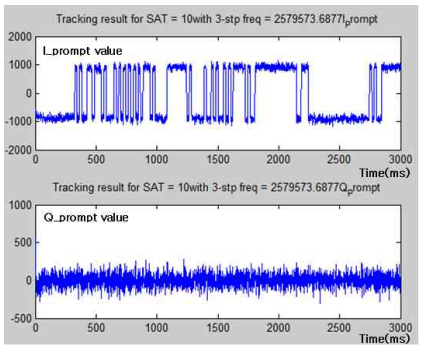


그림 3. 1차 피크에 대한 신호추적 결과(PRN-10)
(위 : I값, 아래 : Q값)
Fig.3. Tracking Result of channel A(PRN-10)
(Top : I, Bottom : Q)

1차 신호획득 이후에 피크의 앞뒤 1/2 chip 구간의 correlation을 평균값으로 대체한 이후 2차 신호획득을 수행한 결과로 1차 신호획득시 두 번째 피크 신호가 검출되는 것을 그림 4에서 확인할 수 있다.

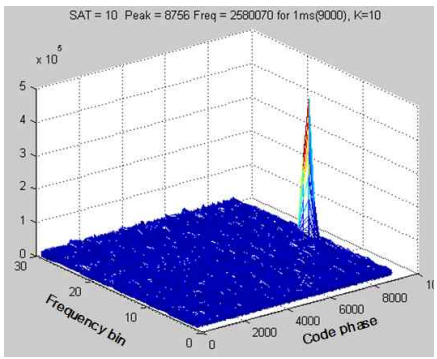


그림 4. 2차 신호획득 결과(PRN-10)
Fig.4. 2nd Acquisition Result(PRN-10)

그림 5는 2차 신호획득 결과로 생성된 채널에서 신호추적을 수행한 결과를 보여주고 있다.

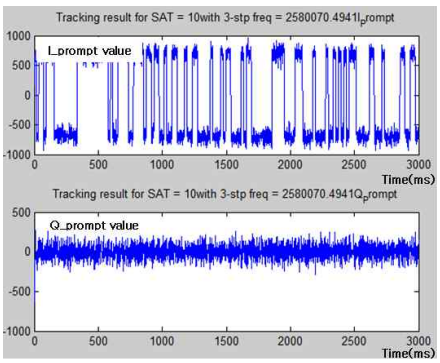


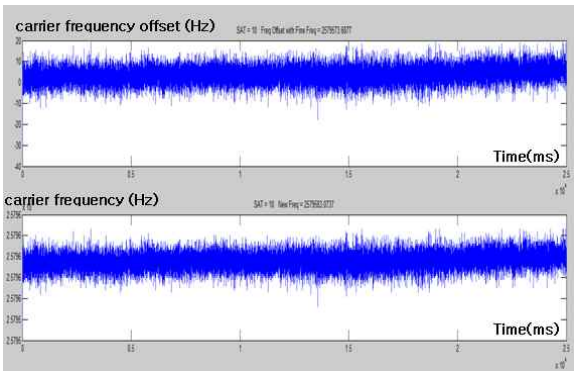
그림 5. 2차 피크에 대한 신호추적 결과(PRN-10)
(위 : I값, 아래 : Q값)
Fig.5. Tracking Result of channel B(PRN-10)
(Top : I, Bottom : Q)

표 2는 전체 신호획득 수행 이후 생성된 두 개의 채널(A,B)에 대한 신호획득 정보를 보여주고 있다.

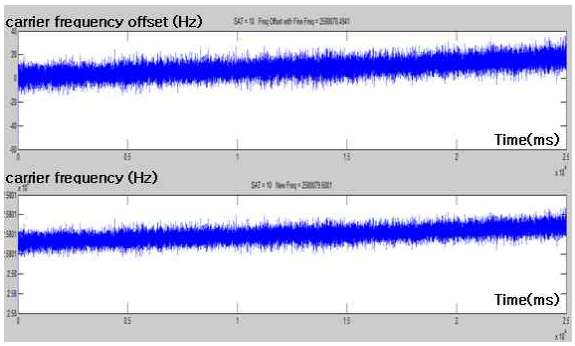
표 2. 이중피크 검출 결과(PRN-10)
Table 2. Result of Double Peak Detection(PRN-10)

Sat	coarse_freq	fine_frequency	code_phase	ratio
10	2579500	2579573	2079	57.4
10	2580000	2580070	8756	35.0

그림 6은 두 개의 채널 A,B에 대하여 20초간 신호추적을 수행하는 동안의 반송파 추적 루프의 오차 변화를 보여주고 있다.



(a) 채널 A의 주파수 변화
(위 : 반송파 추파수 오프셋, 아래 : 반송파 주파수)
(a) Frequency Variation of Channel A
(Top : Carrier Loop offset, Bottom : Carrier Freq.)



(b) 채널 B의 주파수 변화
(위 : 반송파루프 오프셋, 아래 : 반송파 주파수)
(b) Frequency Variation of Channel B
(Top : Carrier Loop offset, Bottom : Carrier Freq.)
그림 6. 신호추적 루프 반송파 변화(PRN-10)
Fig. 6. Carrier Tracking Loop Variation(PRN-10)

A채널은 1차 피크검출과정에서 생성된 결과이고 B채널은 1차 피크를 제거한 이후 2차 신호획득 과정에서 생성된 정보로 생성된 채널이다. 그림에서 위의 그래프는 반송파 주파수 추적 루프의 오차값의 변화를 보여주고 있고 아래 그래프는 신호추적 루프에서의 반송파 값의 변화를 나타내고 있다. GPS신호의 경우 위성의 이동방향에 따라 일정한 비율로 커지거나 작아지는 경향을 보이겠지만 정지되어 있는 기만기의 경우 반송파 추적 루프의 변화량이 상대적으로 작게 되므로 변화율의 차이를 비교하여 기만기 여부를 판단할 수 있다.

그림 7은 A채널과 B채널의 100ms 구간마다 전체 변화율의 평균값을 구한 결과로서 반송파 추적 루프 오차의 평균 변화율을 보여주고 있다. 기울기를 판별하여 그림7의 위 그림은 기만기, 아래그림은 GPS 위성임을 알 수 있다.

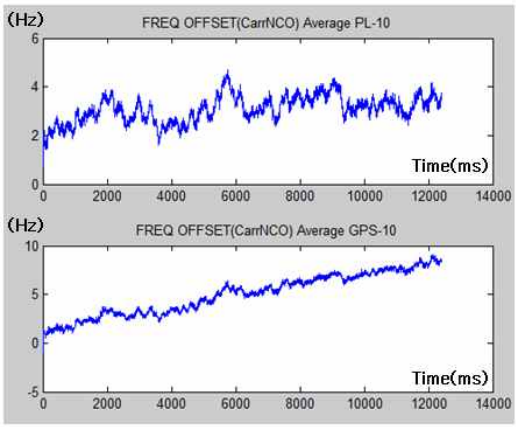


그림 7. 신호추적 반송파루프 평균 변화량(PRN-10)
(위 : A채널, 아래 : B채널)
Fig. 7. Variation Average of Carrier Tracking Loop (PRN-10)
(Top : Channel A, Bottom : Channel B)

신호추적 단계에서 반송파 루프의 측정값으로부터 기만 신호를 판별하여 채널 A, B의 신호추적 결과로 GPS로 판별된 신호에서 추출한 항법데이터를 그림 8에서 확인할 수 있다.

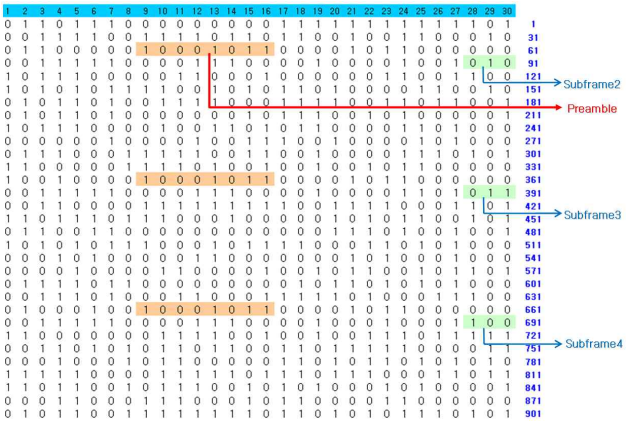


그림 8. 판별된 신호에 대한 데이터 복조 결과 (PRN-10)

Fig.8. Data Decoding Result of Detected Signal

GPS 신호를 기만하기 위해서 기만기의 신호전력이 같은 PRN을 가진 GPS 위성의 신호전력보다 커야 하지만 작을 수도 있으며 이 경우에 대한 예로 위성 PRN 14번의 경우를 살펴본다.

표3과 그림 9는 PRN-14번에 대한 이중피크 검출 결과를 보여주고 있다. 두 개의 피크중 왼쪽의 피크 신호를 2차 신호획득 과정에서 검출하는 것을 확인할 수 있다.

표 3. 이중피크 검출 결과(PRN-14)

Table 3. Result of Double Peak Detection(PRN-14)

Sat	coarse_freq	fine_frequency	code_phase	ratio
14	2579000	2579068	5407	22.2
14	2579500	2579575	3758	19.0

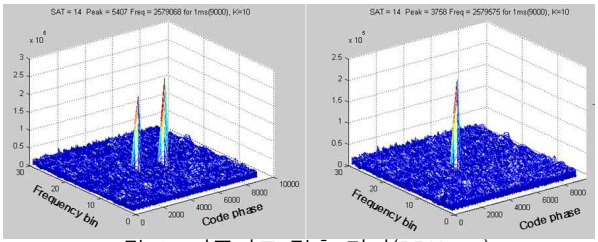
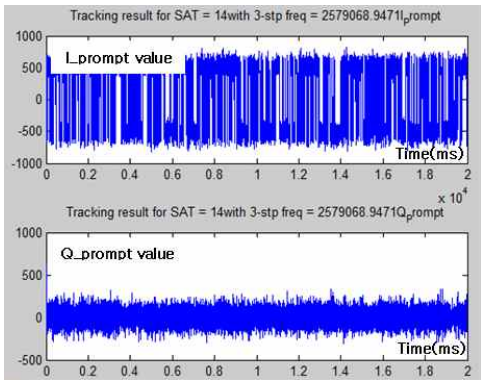


그림 9. 이중피크 검출 결과(PRN-14)

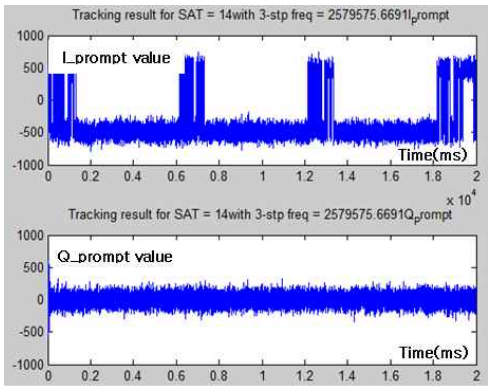
Fig. 9.. Result of Double Peak Detection(PRN-14)

그림 10은 PRN-14번의 두 개의 채널에 대하여 각각 신호추적한 결과를 보여주고 있다.



(a) 1차 신호추적 결과(PRN-14)
(위 : I값, 아래 : Q값)

(a) Tracking Result of channel A(PRN-14)
(Top : I, Bottom : Q)



(b) 2차 신호추적 결과(PRN-14)
(위 : I값, 아래 : Q값)

(b) Tracking Result of channel B(PRN-14)
(Top : I, Bottom : Q)

그림 10. 신호추적 결과(PRN-14)

Fig.10. Tracking Result(PRN-14)

그림 11은 PRN-14번에 대한 반송파 루프의 평균 변화량을 보여주고 있다. PRN-14번의 경우 첫 번째 피크의 신호가 GPS신호인 것을 확인할 수 있다. 이 경우에는 기만신호의 세기가 GPS 신호보다 작은 경우에 해당되고 이러한 경우에도 정상적으로 GPS 신호를 감별하여 선택할 수 있다.

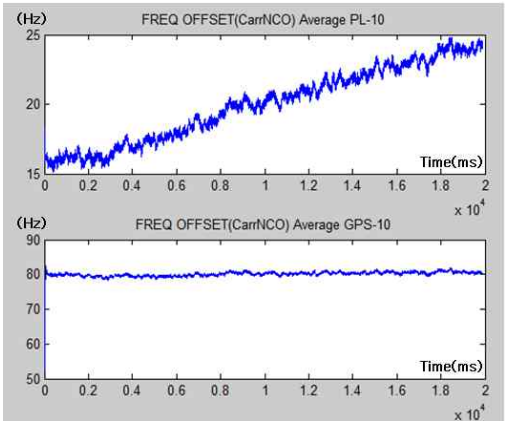


그림 11. 신호추적 반송파루프 평균 변화량(PRN-14)
(위 : A채널, 아래 : B채널)
Fig. 11. Variation Average of Carrier Tracking Loop (PRN-14)
(Top : Channel A, Bottom : Channel B)

V. 결 론

소프트웨어 GPS 수신기를 이용하여 기만신호를 검출하기 위하여 신호획득 단계에서 두 번의 신호획득 과정을 수행함으로서 이중 피크를 검출하고 각각에 대하여 신호추적을 수행하도록 하였다. 이를 위해 의사위성 신호발생기를 이용하여 GPS 위성과 같은 PRN 신호를 발생시키고 Signal-Tap을 이용하여 GPS 신호와 동시에 데이터를 획득하여 소프트웨어 수신기를 이용하여 실험한 결과 신호획득 단계에서 하나의 PRN에 대하여 두 개의 피크를 가진 신호를 확인할 수 있었고 첫 번째 피크 신호의 1-chip이내의 상관값을 평균값으로 대체한 후 2차 신호획득 과정을 수행하는 방법을 이용하여 두 번째 피크 신호의 정보를 획득 할 수 있었다. 둘 중에 강한 신호만을 추적하였던 기존의 수신기와 달리 두 신호에 대해 모두 신호추적을 수행한 다음 반송파 루프 측정값을 이용하여 기만신호의 데이터가 아닌 본래의 GPS 데이터를 복조할 수 있었다. 그리고 기만신호가 GPS 신호보다 약한 경우에도 일반적인 수신기와 마찬가지로 정상적인 GPS 신호 활용이 가능한 것을 확인할 수 있었다. 이러한 방식을 사용하면 기존의 기만신호 감별 단계 이후에 해당 위성 신호를 배제하는 대응기법과 달리 해당 PRN에 대한 위성 정보에 대한 손실을 피할 수 있게 된다. 이를 활용하면 다중 기만신호에 대해서도 대처가 가능하다. 추후로는 기만신호의 세기 변화나 수신기의 이동에 따라 신호추적 단계에서 추가적인 감별기법을 적용한 대응 기법에 대한 연구가 필요하다.

감사의 글

본 논문은 2012년 국토해양부 소관 연구개발사업의 연구비 지원에 의해 수행되었습니다.

Reference

[1] Mi-young Shin, Sung-Lyong Cho, Jun-Oh Kim, ki-Won Song, Sang-Jeong Lee, “Analysis of GPS Spoofing Characteristics and Effects on GPS Receiver”, *The Korea Institute of Military Science and Technology,* vol. 13, no. 2, 2010. 4, pp. 296-303.

[2] SungLyong Cho MiYoung Shin, SangJeong Lee, Chansik Park, "Performance Comparison of Anti-Spoofing Methods using Pseudorange Measurements”, *The Korea Institute of Military Science and Technology,* vol13, no 5, pp.793~800, 2010.10

[3] H. Wen, P. Y. Huang, J. Dyer, A. Archinal and J.Fagan, “Countermeasures for GPS signal spoofing”, *Proc. of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation,* pp. 1285~1290, 2005.

[4] T.E. Humphreys et al., “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” *ION GNSS Conf.*, 2008.

[5] S.K Jeong, Taehee Kim, Cheon Sig Sin, Sanguk Lee, "Technical Trends of Smart Jamming for GPS Signal", *Electronics and Telecommunications Trends,* vol 27, no 6, 2012.12

[6] Taehee Kim, Cheon Sig Sin, Sanguk Lee, "Analysis of Effect of Spoofing Signal According to Code Delay in GPS L1 Signal", *The Korea Society of Space Technology,* vol 7, no 1, 2012.06

[7] Sung-Hyuck Im, Jun-Hyuk Im, Jong-Hwa Song, "Susceptibility of Spoofing On A GPS L1 C/A Signal Tracking Loop", *The Korean Navigation Institute,* vol 15, 2011.02

권 금 철(Keum-Cheol Kwon)

2001년 중앙대 전자전기공학부 공학사,
2003년 중앙대 전자전기공학부 공학석사,
2007년~현재 중앙대 전자전기공학부 박사 과정
관심분야 : 컴퓨터, 반도체, SOC 설계, GPS

양 철 관 (Cheol-Kwan Yang)

1996년 중앙대 제어계측공학과 공학사,
1998년 중앙대 전자전기공학부 공학석사,
2003년 중앙대 전자전기공학부 공학박사,
현재 (주)피에스키시스템즈, 책임 연구원,
관심분야 : 고장검출, 항법알고리즘, GPS, 강인필터.

심 덕 선 (Duk-Sun Shim)

1984년 서울대 제어계측공학과 공학사
1986년 서울대 제어계측공학과 공학석사
1993년 미시간대 항공우주공학과 공학박사
1995년 3월~현재 중앙대학교 전자전기 공학부 교수,
관심분야 : 제어, GPS, 관성항법시스템, 필터링, 고장검출.